We claim:

1. A method for producing an elliptic curve point multiplication product, $Q = eP$, using an arbitrary integer e, a point P on an elliptic curve group G defined over a field F, where $G \subset F \times F$, comprising the steps of:

constructing a set G';

constructing a mapping T from G into the set G', constructing a mapping T^{-1} from G' onto G, and constructing an operation $\oplus$ defined on G', such that (a) given $P \in G$, $T^{-1}(\, T(P)\,) = P$, and (b) $P + P = T^{-1}(P' \oplus P')$, where $P' = T(P)$;

producing an elliptic curve point multiplication product Q by transforming the point P to the point P' using the mapping T, performing the operation $\oplus$ on the point P' to determine the point $Q' = e\,P'$, transforming the point Q' to the product Q using the mapping T^{-1}; and

using the product Q in a cryptographic operation.

2. The method of claim 1 wherein the set G, the set G', the mapping T, the operation $\oplus$, and the mapping T^{-1} are constructed such that given $P_1, P_2, \ldots, P_N \in G$, where N is an integer, the computation of $T^{-1}(\, T(P_1) \oplus T(P_2) \oplus \ldots \oplus T(P_N))$ is more efficient than the computation of $P_1 + P_2 + \ldots + P_N$.

3. The method of claim 1 wherein:

the mapping T is constructed by selecting any element r of the field F, and defining T as $T: (x, y) \rightarrow (x \cdot r, y \cdot r)$, where $P = (x, y) \in G$, and $\cdot$ is the multiplication operator in F; and

the mapping T is constructed by defining $T: (u,v) \rightarrow (u \cdot r^{-1}, v \cdot r^{-1})$, where $P' = (u,v) \in G'$.

4. The method of claim 3 wherein the field F is a member of GF(p).

5. The method of claim 4 wherein the element r is selected as the smallest power of 2 that is larger than p.

6. The method of claim 4 wherein the element r is selected as the product of prime numbers.

7. The method of claim 4 wherein the operation $\oplus$ is constructed such that the addition of two points in the set G' is given by:

$(x_3', y_3') = (x_1', y_1') \oplus (x_2', y_2')$;

$z' = (x_2' - x_1')^{-1} \cdot r^2$;

$L' = (y_2' - y_1') \cdot z' \cdot r^{-1}$;

$x_3' = L' \cdot L' \cdot r^{-1} - x_1' - x_2'$; and

$y_3' = L' \cdot (x_1' - x_3') \cdot r^{-1} - y_1'$.

8. The method of claim 4 wherein the operation $\oplus$ is constructed such that the doubling of a point in the set G' is given by:

$(x_1', y_1') \oplus (x_1', y_1') = (x_3', y_3')$;

$z' = (y_1' + y_1')^{-1} \cdot r^2$;

$L' = ((x_1' + x_1' + x_1') \cdot x_1' \cdot r^{-1} + a) \cdot z' \cdot r^{-1}$;

$x_3' = L' \cdot L' \cdot r^{-1} - x_1' - x_1'$; and

$y_3' = L' \cdot (x_1' - x_3') \cdot r^{-1} - y_1'$.

9. The method of claim 4 wherein the Montgomery Algorithm in GF(p) is utilized to perform the operation $\oplus$ on the point P' to determine the point $Q' = eP'$.

10. The method of claim 3 wherein the field F is a member of $GF(2^k)$.

11. The method of claim 10, wherein the operation $\oplus$ is constructed such that the addition of two points in the set G' is given by:

$$(x_3', y_3') = (x_1', y_1') \oplus (x_2', y_2');$$

$$z' = (x_1' + x_2')^{-1} \cdot r^2;$$

$$L' = (y_1' + y_2') \cdot z' \cdot r^{-1};$$

$$x_3' = (L' \cdot L' \cdot r^{-1}) + L' + x_1' + x_2' + a'; \text{ and}$$

$$y_3' = (L' \cdot (x_1' + x_3') \cdot r^{-1}) + x_3' + y_1'.$$

12. The method of claim 10, wherein the operation $\oplus$ is constructed such that the doubling of a point is given by:

$$(x_1', y_1') \oplus (x_1', y_1') = (x_3', y_3');$$

$$z' = (x'_1)^{-1} \cdot r^2;$$

$$x_3' = x_1' \cdot x_1' \cdot r^{-1} + (z' \cdot z' \cdot r^{-1}) \cdot b \cdot r^{-1}; \text{ and}$$

$$y_3' = x_1' \cdot x_1' \cdot r^{-1} + (x_1' + y_1' \cdot z' \cdot r^{-1}) \cdot x_3' \cdot r^{-1} + x_3'.$$

13. The method of claim 10 wherein the element r is selected as $x^k \bmod n(x)$, where $n(x)$ is the irreducible polynomial generating the field $GF(2^k)$.

14. The method of claim 10 wherein the Montgomery Algorithm in $GF(2^k)$ is utilized

to perform the operation $\oplus$ on the point P' to determine the point $Q' = e\,P'$.

15. The method of claim 1 wherein the step of performing the operation $\oplus$ on the point P' utilizes a binary method.

16. The method of claim 1 wherein the step of performing the operation $\oplus$ on the point P' utilizes an M–ary method.

17. The method of claim 1 wherein the elements of sets G and G' are implemented using Projective Coordinates.

18. A method for optimizing the calculation of an expression $f = f(x_1, \ldots, x_i, \ldots, x_n)$, wherein the expression f is comprised of a finite number of arbitrary field operations over any finite field F, and $x_1, \ldots, x_i, \ldots, x_n$ are all elements of F, comprising the steps of:

selecting an element r, a constant, from the field F;

transforming the expression $f = f(x_1, \ldots, x_i, \ldots, x_n)$ to the $f' = f'(x_1', \ldots, x_i', \ldots, x_n')$ by

replacing all occurrences of x in the expression f with x', giving f_1, where x denotes a variable or constant of f;

replacing all occurrences of $x \cdot y$ in the expression f_1 with $x \otimes y$, giving f_2, where x and y denote subexpressions of f_1;

replacing all occurrences of x^{-1} in the expression f_2 with $x^{-1} \cdot r^2$, giving f_3, where x denotes a subexpression of f_2;

replacing all occurrences of $x \otimes y$ in the expression f_3 with $x \cdot y \cdot r^{-1}$, giving f_4, where x and y denote subexpressions of f_3; and

replacing all occurrences of x' in the expression f_4 with $x \cdot r$, giving f', where x denotes a primed variable or primed constant in f_4;

determining $f = f' \cdot m^{-1}$; and

using $f' \cdot m^{-1}$ to calculate f in a cryptographic operation.

19. The method of claim 18 wherein each instance of $x' \cdot y' \cdot m^{-1}$ is computed using the Montgomery Algorithm when the set F is a member of GF(p).

20. The method of claim 18 wherein each instance of $x' \cdot y' \cdot m^{-1}$ is computed using the Montgomery Algorithm in $GF(2^k)$ when the set F is a member of $GF(2^k)$.

21. A method for producing an elliptic curve point addition product, $Q = P + P$, using a point P on an elliptic curve group G defined over a field F, where $G \subset F \times F$, comprising the steps of:

constructing a set G';

constructing a mapping T from G into the set G', constructing a mapping T^{-1} from G' onto G, and constructing an operation $\oplus$ defined on G', such that (a) given $P \in G$, $T^{-1}(T(P)) = P$, and (b) $P+P = T^{-1}(P' \oplus P')$, where $P' = T(P)$; and

producing an elliptic curve point addition product Q by transforming the point P to the point P' using the mapping T, performing the operation $\oplus$ on the point P' and the point P' to determine the point Q', transforming the point Q' to the product Q using the mapping T^{-1}; and using the product Q in a cryptographic operation.

22. A method for producing an elliptic curve point addition product, $Q = P + S$, using

points P and S on an elliptic curve group G defined over a field F, where $G \subset F \times F$, comprising the steps of:

constructing a set G';

constructing a mapping T from G into the set G', constructing a mapping T^{-1} from G' onto G, and constructing an operation $\oplus$ defined on G', such that (a) given $P \in G$, $T^{-1}(\ T(P)\ ) = P$, and (b) $P+S = T^{-1}(P' \oplus S')$, where $P' = T(P)$ and $S' = T(S)$; and

producing an elliptic curve point addition product Q by transforming the point P to the point P' using the mapping T, by transforming the point S to the point S' using the mapping T, performing the operation $\oplus$ on the point P' and the point S' to determine the point Q', transforming the point Q' to the product Q using the mapping T^{-1}; and

using the product Q in a cryptographic operation.

23. Apparatus for producing an elliptic curve point multiplication product, $Q = eP$, using an arbitrary integer e, a point P on an elliptic curve group G defined over a field F, where $G \subset F \times F$, comprising:

means for constructing a set G';

means for constructing a mapping T from G into the set G', constructing a mapping T^{-1} from G' onto G, and constructing an operation $\oplus$ defined on G', such that (a) given $P \in G$, $T^{-1}(\ T(P)\ ) = P$, and (b) $P+P = T^{-1}(P' \oplus P')$, where $P' = T(P)$; and

means for producing an elliptic curve point multiplication product Q by transforming the point P to the point P' using the mapping T, performing the operation $\oplus$ on the point P' to determine the point $Q' = e\,P'$, transforming the point Q' to the product Q using the mapping T^{-1}; and

means for using the product Q in a cryptographic operation.